MDJ:rfb 4/25/00 245-53435

#7

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53435	App:
	Applicant: Çetin K. Koç, Erkay Savaş	
	Filed:	Art Unit:

jc682 U.S. PTO 09/558138 04/25/00

OTHER DOCUMENTS

		✓	B. S. Kaliski, Jr., "The Montgomery Inverse and Its Applications," IEEE Transactions on Computers 44:1064-1065 (August 1995)
		✓	P. L. Montgomery, "Modular Multiplication Without Trial Division," Mathematics of Computation 44:519-521 (April 1985)
		✓	Ç. K. Koç et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro 16:26-33 (June 1996)
		✓	J. Dhem et al., "SCALPS: Smart Card For Limited Payment Systems," IEEE Micro 16:42-51 (June 1996)

EXAMINER: Joseph M. McCloy DATE: 11-24-03

*Examiner: Initial if considered, whether or not in conformance with MPEP 60; draw line through cite if not in conformance and not considered. Send copy.

MJ:mgs 07/01/2002 245-53435 123983.doc

RECEIVED
JUL 11 2002
Technology Center 2600

#8

OIPE JUL 08 2002 PATENT & TRADEMARK OFFICE

RECEIVED
JUL 12 2002
Technology Center 2100

INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Docket: 245-53435	App: 09/558,138
	Applicant: Koc et al.	
	Filed: April 25, 2000	Art Unit: 2685

OTHER DOCUMENTS

		/	Menezes, et al., Handbook of Applied Cryptography, p. 600-603 (CRC Press 1997).
		/	S. Even, "Systolic Modular Multiplication," Advances in Cryptology, Lecture Notes in Computer Science **537**:619-624 (Springer Verlag 1990).
		/	Bosselaers et al., "Comparison of Three Modular Reduction Functions," Crypto '93, pp. 175-186 (1993).
		/	Koc et al., "Carry-save Adders for Computing the Products AB Modulo N," Electronics Letters **26**:899-900 (June 21, 1990).
		/	C.K. Koc., "Montgomery Reduction with Even Modulus," IEEE Proc.-Compt. Digit Tech., **141**:314-316 (September 5, 1994).
		/	Paar et al., "Fast Arithmetic Architectures for Public-Key Algorithms over Galois Fields $GF((2^n)^m)$," Eurocrypt '97, p. 363-378 (May 11, 1997).
		/	Leu et al., "A Scalable Low-Complexity Digit-Serial VLSI Architecture for RSA Cryptosystem." SiPS 99 IEEE Workshop on Signal Processing Systems, p. 586-595 (1999).
		/	Bartee et al., "Computation with Finite Fields," Information and Control **6**:79-98 (1963).
		/	C.D. Walter, "Faster Modular Multiplication by Operand Scaling," Advances in Cryptology: Lecture Notes in Computer Science **576**:313-323 (1992).
		/	Bajard, et al., "An RNS Montgomery Modular Multiplication Algorithm," IEEE Trans. on Computers, **47**:766-776 (July 1998).
		/	Koc et al., "Montgomery Multiplication in $GF(2^k)$," Designs, Codes and Cryptography, **14**:57-69 (April 1998).
		/	G.B. Agnew et al., "Arithmetic Operations in $GF(2^m)$," Journal of Cryptology, p. 3-13 (1993).

EXAMINER: Joseph M McArdle	DATE 11-24-03

*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.